SSE-CMM Security Metrics

George Jelen, Chairman

Profiles, Assurance and Metrics Committee

International Systems Security Engineering Association

ISSEA
International Systems Security Engineering Association

Briefing Outline

- A brief review of the history of the SSE-CMM project
- A look at the SSE-CMM appraisal as a metric
- Description of three specific project efforts
  - 1999 conference paper
  - Ongoing document drafting effort
  - IATAC current research effort

Brief History of the SSE-CMM Project

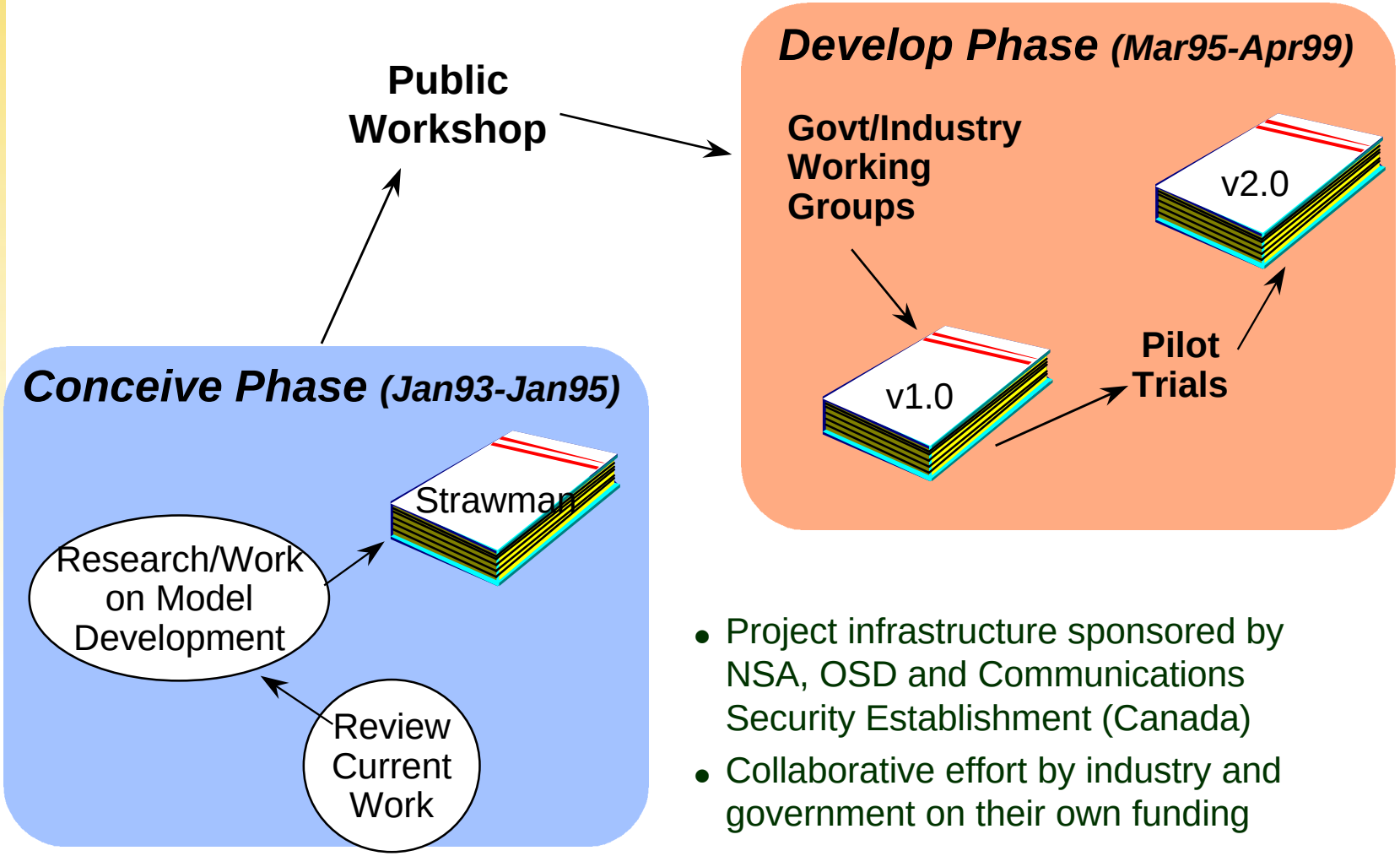
ISSEA
International Systems Security Engineering Association

Why was the SSE-CMM developed?

- Objective:
  - advance security engineering as a defined, mature, and measurable discipline
- Project Goal:
  - Develop a mechanism to enable:
    - selection of appropriately qualified security engineering providers
    - focused investments in security engineering best practices
    - capability-based assurance

ISSEA
International Systems Security Engineering Association

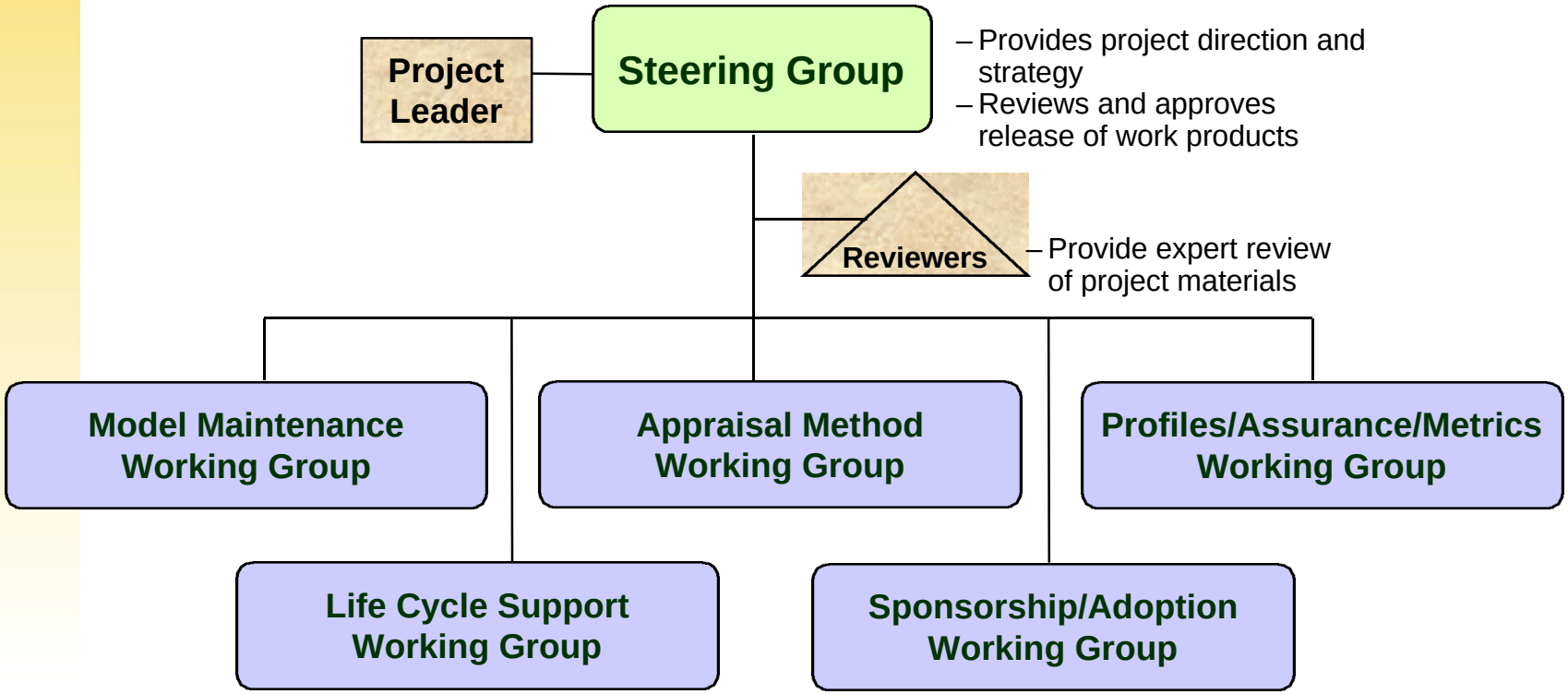
Project History



- Project infrastructure sponsored by NSA, OSD and Communications Security Establishment (Canada)
- Collaborative effort by industry and government on their own funding

ISSEA
International Systems Security Engineering Association

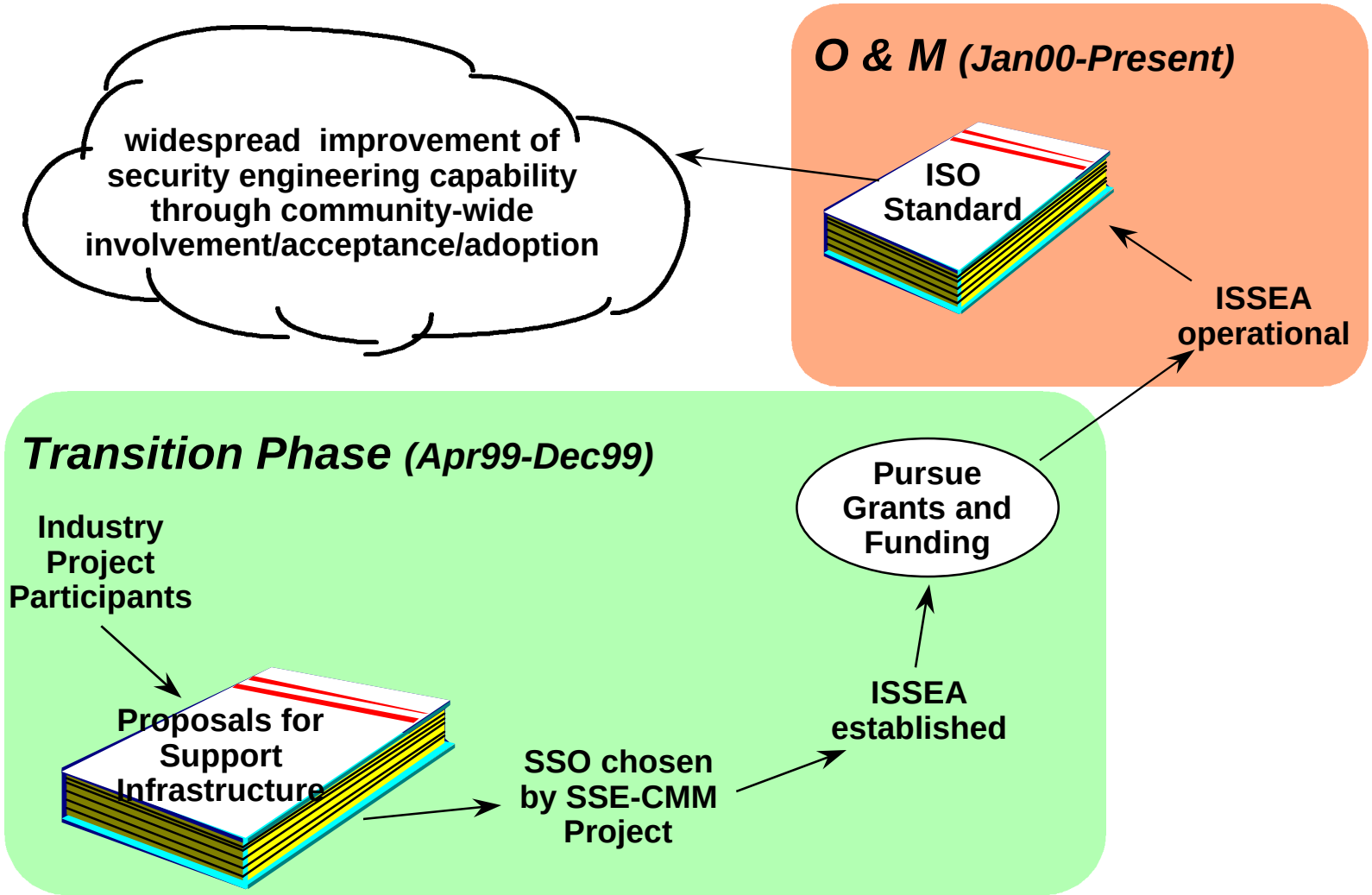
Project Structure



- Original work and project infrastructure sponsored by NSA; additional support provided by OSD and Communications Security Establishment (Canada)
- Collaborative effort by industry and government on their own funding

ISSEA
International Systems Security Engineering Association

The Current Path



SSO = SSE-CMM Support Organization ISSEA = International Systems Security Engineering Association

ISSEA
International Systems Security Engineering Association

ISSEA Objectives

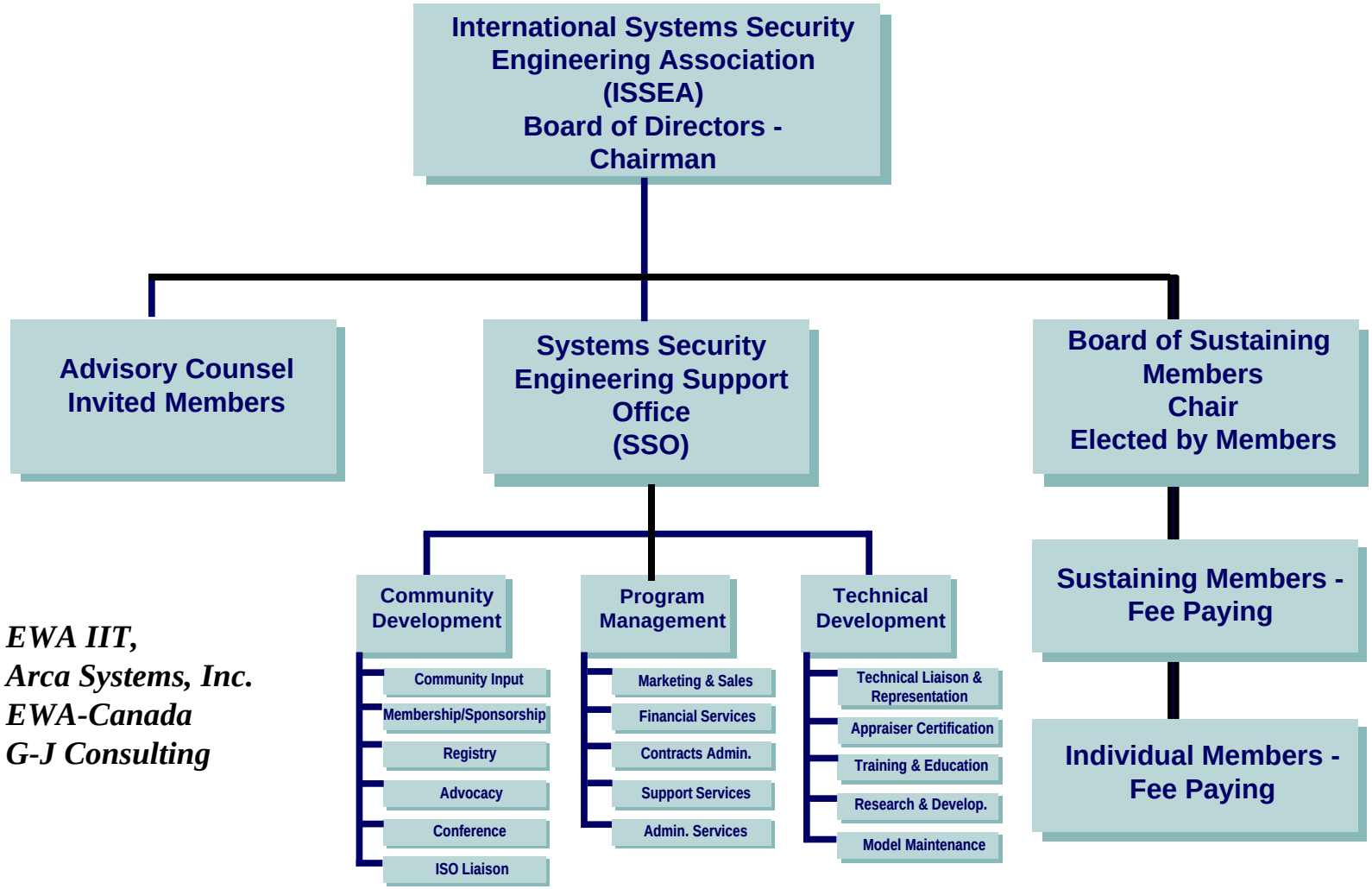
- Establish systems security engineering as a defined and measurable discipline
- Accomplish ISO standard to gain worldwide acceptance of the SSE-CMM
- Provide for maintenance of the SSE-CMM
- Promote the adoption of the SSE-CMM

ISSEA
International Systems Security Engineering Association

What is the ISSEA?

- Not for profit professional organization
- Oversees SSO in furthering development and use of the SSE-CMM
- Receives advice and guidance from Advisory Council and Board of Sustaining Members

ISSEA Organization



SSO = EWA IIT,
Arca Systems, Inc.
EWA-Canada
G-J Consulting

The SSE-CMM Appraisal as a Metric

ISSEA
International Systems Security Engineering Association

What is the SSE-CMM?

- Describes those characteristics of a security engineering process essential to ensure good security engineering
- Does not prescribe a particular process or sequence
- Captures industry's best practices

ISSEA
International Systems Security Engineering Association

How does the SSE-CMM define best practices?

- Domain Aspect
  - process areas
  - base practices
- Capability Aspect
  - implementation of process areas
  - institutionalization of process areas

ISSEA
International Systems Security Engineering Association

SSE-CMM Base Architecture

- **Three Domain Categories**
  - Organization
  - Project
  - Security Engineering
- **Five Capability Levels**
  - Performed Informally
  - Planned and Tracked
  - Well Defined
  - Quantitatively Controlled
  - Continuously Improving

ISSEA
International Systems Security Engineering Association

SSE-CMM Organization Process Areas

- Define Organization's Security Engineering Process
- Improve Organization's Security Engineering Process
- Manage Security Product Line Evolution
- Manage Security Engineering Support Environment
- Provide Ongoing Skills and Knowledge
- Coordinate with Suppliers

ISSEA
International Systems Security Engineering Association

SSE-CMM Project Process Areas

- Ensure Quality
- Manage Configurations
- Manage Program Risk
- Monitor and Control Technical Effort
- Plan Technical Effort

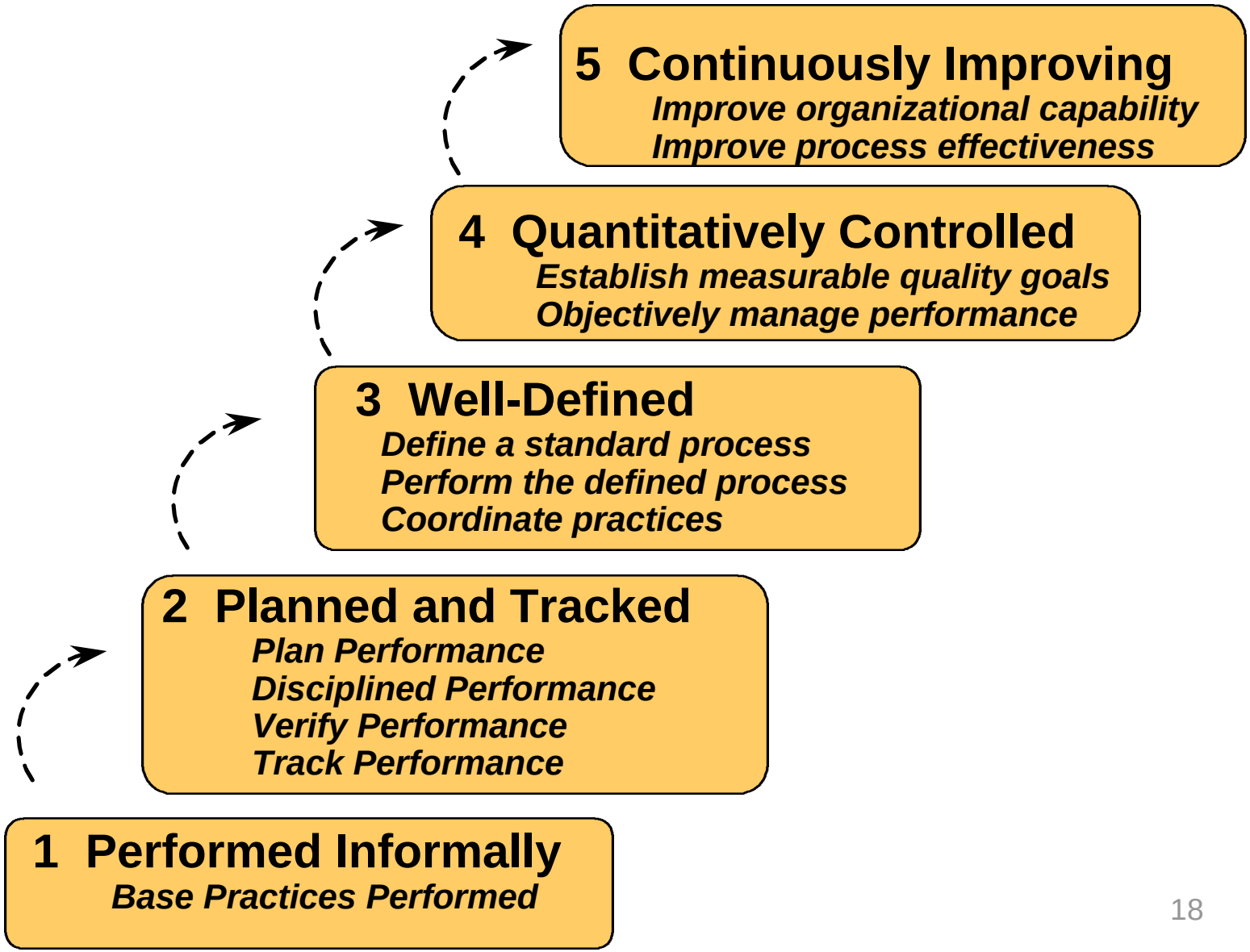
ISSEA
International Systems Security Engineering Association

SSE-CMM Security Engineering Process Areas

- Administer Security Controls
- Assess Impact
- Assess Security Risk
- Assess Threat
- Assess Vulnerability
- Build Assurance Argument
- Coordinate Security
- Monitor Security Posture
- Provide Security Input
- Specify Security Needs
- Verify and Validate Security

ISSEA
International Systems Security Engineering Association

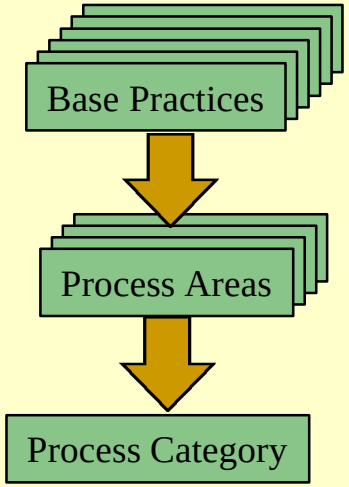
Organizational Capability Measures



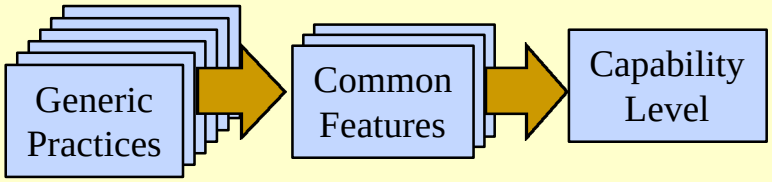
ISSEA
International Systems Security Engineering Association

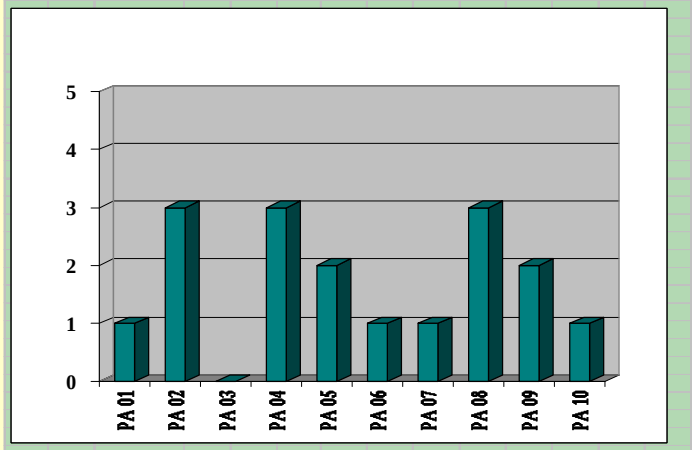
SSE-CMM Model Architecture

Domain



Capability





ISSEA
International Systems Security Engineering Association

The SSE-CMM Appraisal Method

- Uses a standard process
- Clearly defines team member roles
- Yields a rating profile
- Produces significant findings

ISSEA
International Systems Security Engineering Association

Appraisal Method Phases

- Planning phase
- Preparation phase
- Onsite phase
- Reporting phase

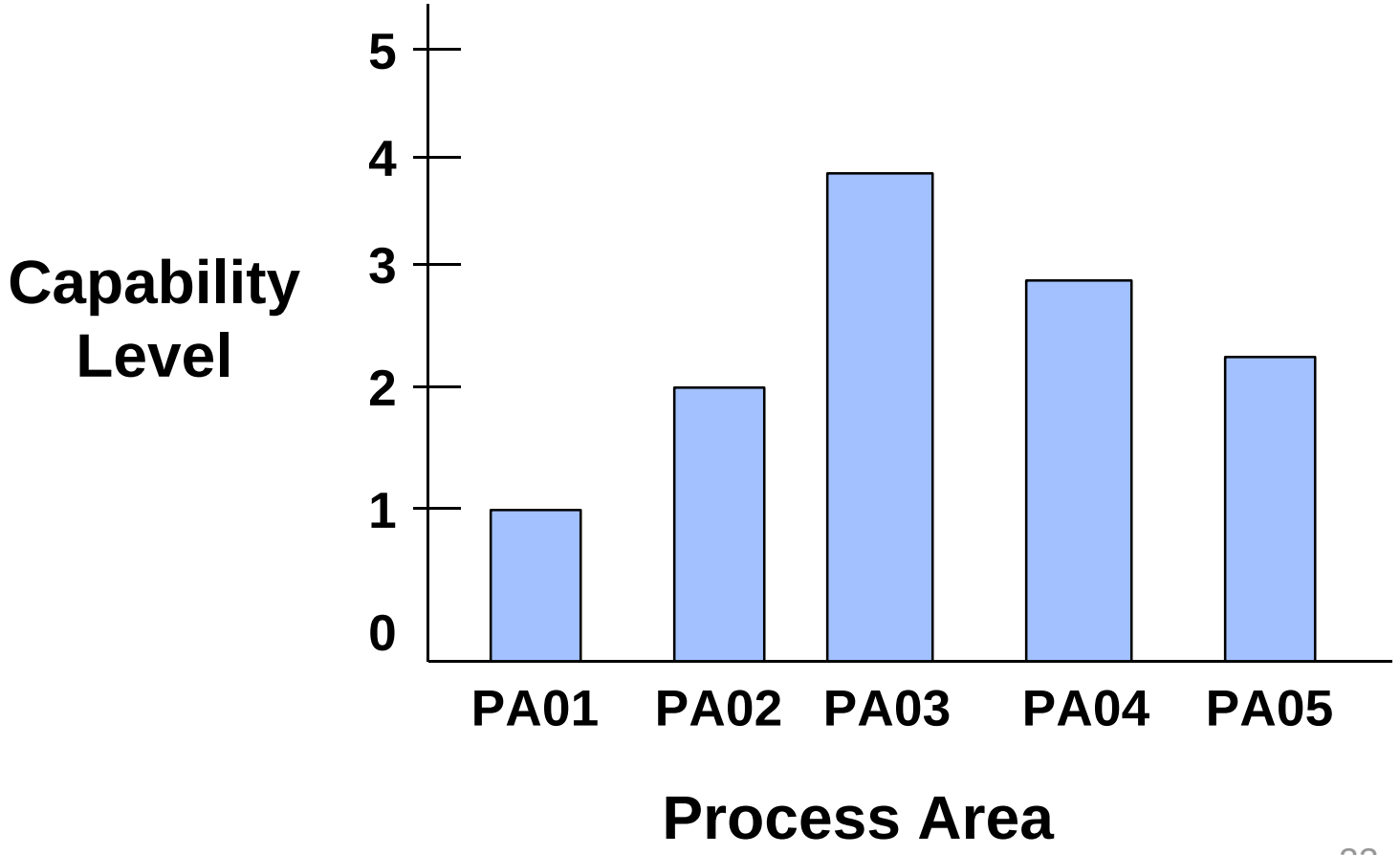
ISSEA
International Systems Security Engineering Association

Appraisal Process

- Administer questionnaire
- Conduct targeted interviews
- Fill in data tracking sheet
- Develop preliminary findings
- Perform follow-up interviews
- Produce rating profile and final findings

ISSEA
International Systems Security Engineering Association

The Rating Profile



ISSEA
International Systems Security Engineering Association

Major Uses of the SSE-CMM Appraisal

- Third-party appraisals for source selection purposes
- Internal self appraisals for self improvement

Internal Metrics Efforts of the SSE-CMM Project

ISSEA
International Systems Security Engineering Association

Why the SSE-CMM Project Involved Itself With Metrics

- To provide appraisal evidence
- To validate the utility of the model

ISSEA
International Systems Security Engineering Association

Guiding Principles

- You have to do it before you can manage it
- Understand what's happening on the project before defining organization-wide processes
- You can't measure it until you know what “it” is
- Managing with measurement is only meaningful when you're measuring the right things
- A culture of continuous improvement requires a foundation of sound management practice, defined processes, and measurable goals

ISSEA
International Systems Security Engineering Association

Two Types of Metrics

- Process Metric—Some measure that could be offered as evidence of the maturity of some SSE-CMM Process Area
- Security Metric—Some way of indicating the extent to which some security attribute, i.e., confidentiality, integrity, etc., is present

ISSEA
International Systems Security Engineering Association

Internal Metrics Efforts

- 1999 conference paper
- Ongoing document drafting effort
- IATAC current research effort

ISSEA
International Systems Security Engineering Association

1999 Conference Paper

- Systems Security Engineering Conference, February 3-4, 1999
- Paper Title – "Developing and Applying System Security Engineering Metrics"
- Authors – Nadya Bartol, Lisa Gallagher, and Natalie Givans
- Paper summarized the Metrics Action Committee's early work and presented an approach to metrics development

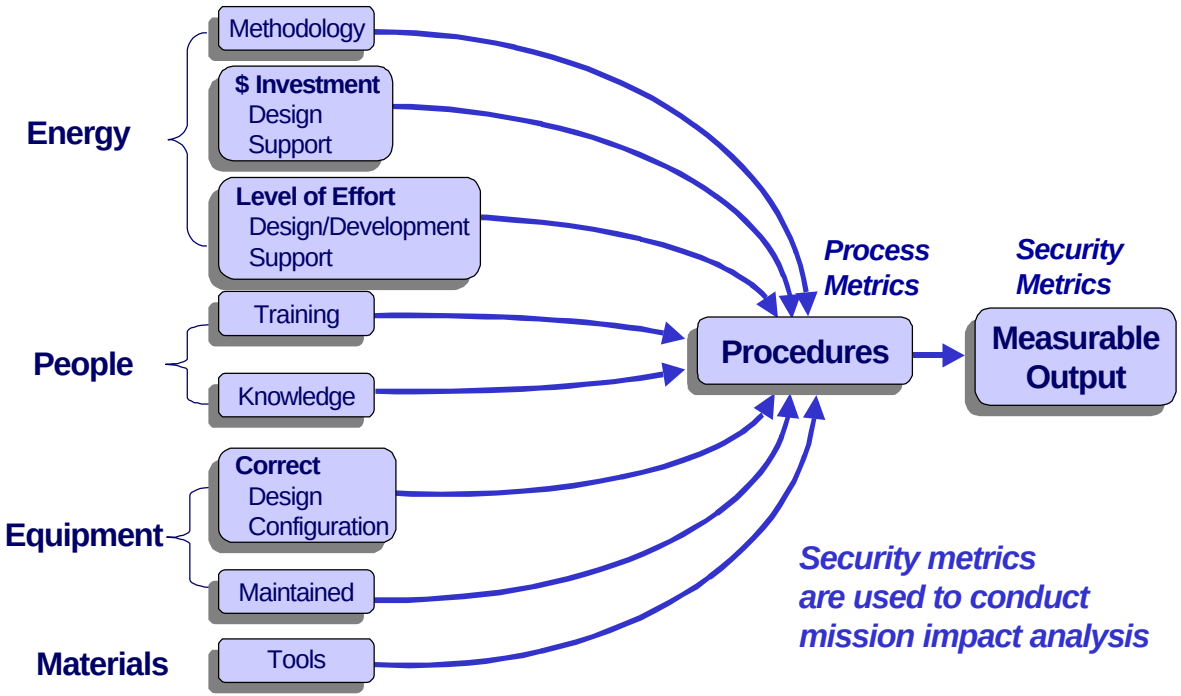
ISSEA
International Systems Security Engineering Association

Committee's Definition of Process

"The logical organization of people, material, energy, equipment, and procedures into work activities designed to produce a specified end result."

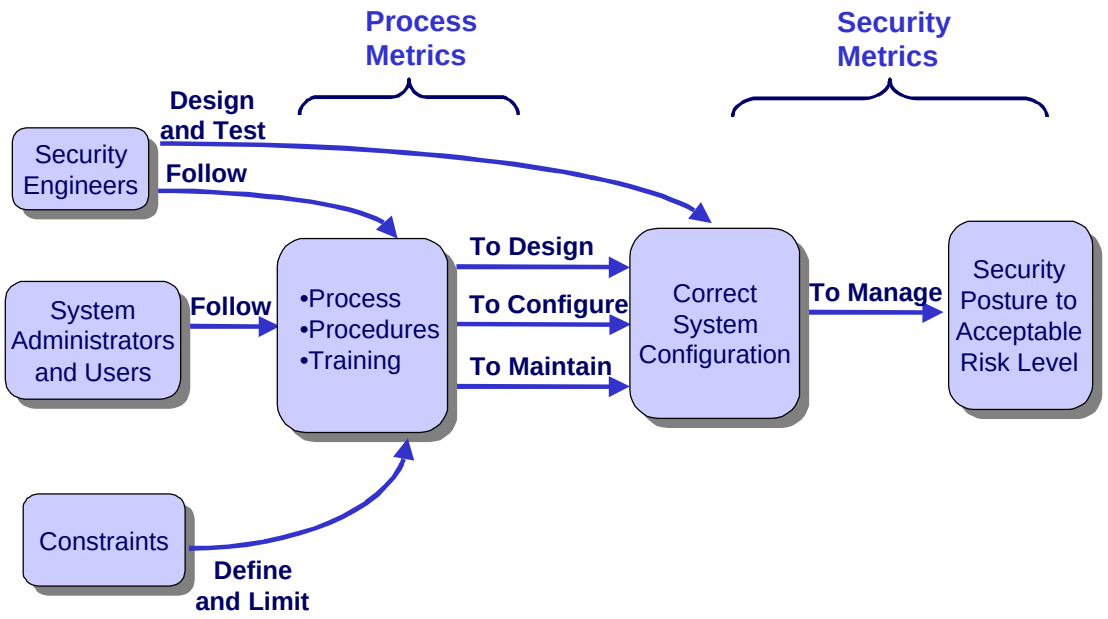
ISSEA
International Systems Security Engineering Association

A Metrics Development Process



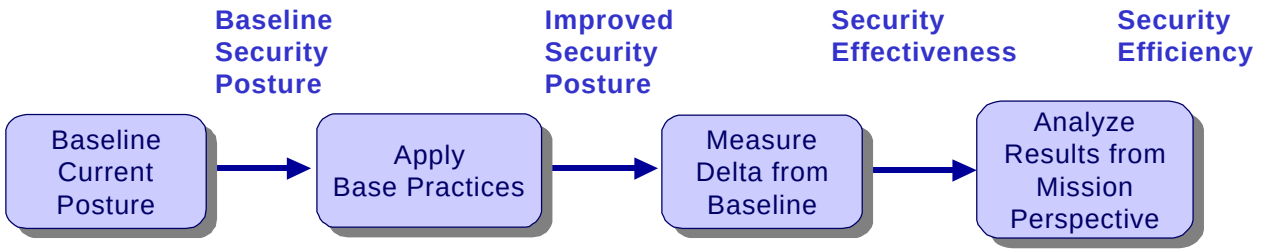
ISSEA
International Systems Security Engineering Association

Relationship Between Process and Security Metrics



ISSEA
International Systems Security Engineering Association

Applying Process and Security Metrics



- Process Metrics
- Security Metrics

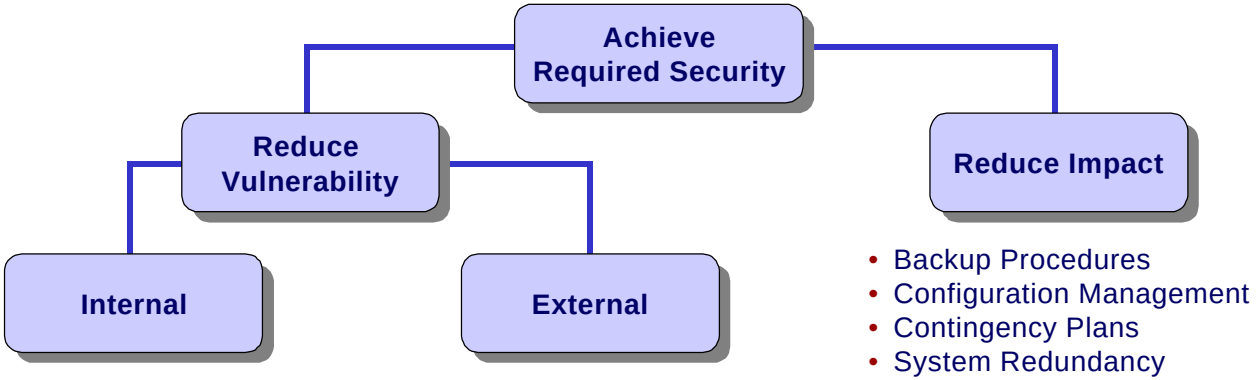
- Risk Assessment
- Security Engineering
- Project and Organizational BPs

- Process Metrics
- Security Metrics

- Cost-Benefit Analysis
- Return on Investment
- Operational Effectiveness

ISSEA
International Systems Security Engineering Association

Top-Down Tree



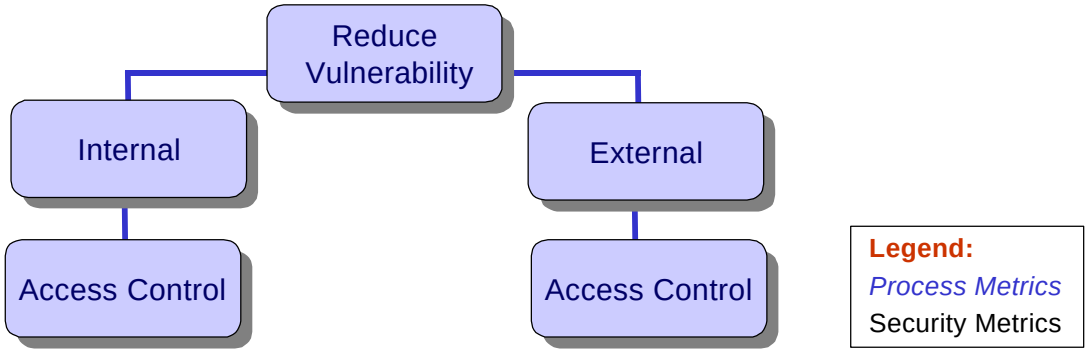
- Backup Procedures
- Configuration Management
- Contingency Plans
- System Redundancy

- **Access Control**
- Accountability
- Audit
- Authentication
- Availability
- Configuration Management
- Detection
- Education and Awareness
- Monitoring
- Policy and Procedures
- Standard Design Processes

- **Access Control**
- Audit
- Detection
- Monitoring

ISSEA
International Systems Security Engineering Association

Sample Metrics for Access Control



- ***Frequency of regular audit reviews***
- ***Percent of users with passwords meeting policy***
- **No. of failed login attempts**
- **No. of virus infections per month**
- **Frequency and compliance with virus detection updates**
- **No. of infected components per virus incident (measures response)**
- **Frequency of audit reviews**

- ***Percent of externally exposed systems with intrusion detection system***
- ***No. of firewalls per external access point***
- ***No. of external users required to use strong identification and authentication (I&A)***
- **Time elapsed between discovery of intrusion and initiation of corrective measures**
- **Percent range and number of successful external network penetrations over a specific time period**
- **No. of system accesses by unauthorized users through channels protected by strong I&A**

ISSEA
International Systems Security Engineering Association

One Company's Experience

- Process metrics are more useful than security metrics in assessing process maturity
- Performing a self assessment, using measurements, does yield quantifiable efficiencies and cost savings

ISSEA
International Systems Security Engineering Association

Specific Realized Process Efficiencies

- Decreased the time required to conduct a Security Test and Evaluation (ST&E) of identical network components at different sites eight times between the first and nth efforts
- Reduced site visits by three people lasting five days in Phase 1 of a large three-phase risk assessment effort to visits by two people for three days in Phase 2

ISSEA

International Systems Security Engineering Association

Ongoing Document Drafting Effort

ISSEA
International Systems Security Engineering Association

Documents in Preparation

- "CIO Metrics for Information Assurance"
- "SSE-CMM Practitioners Guide to Applying Metrics in Support of Business operations"

ISSEA
International Systems Security Engineering Association

Both Documents Based Upon GMITS

- Corporate Information Assurance Metrics – traced to Corporate Security Policy
- Corporate IT Information Assurance Metrics – traced to Corporate IT Security Policy
- IT System Information Assurance Metrics – traced to IT System Security Policy

ISSEA
International Systems Security Engineering Association

CIO Document

- Intended for Chief Information Officers
- Aimed at a broad understanding
- Based on the application of widely available standards and procedures

ISSEA
International Systems Security Engineering Association

Business Issues and Concerns

Business Issue	Management Concerns
Fiduciary Responsibilities	- Due Diligence - Liability
Trust relationships with external organizations and clients	Strategic alliances Joint ventures Outsourcing partners
Public Image and Litigation	Fraud & Deception Reputation
Loss of Control	Internal Information Need-to-know External access to sensitive internal information
Loss of Intellectual Property and Business Opportunities	Industrial Espionage Corporate intelligence gathering Hostile takeovers
Increased operating costs Reduced production capacity	Productivity losses Frozen or unavailable information assets
Loss of product-related income	Product risks (concepts, design information, drawings, patents, etc.)
Loss of service-related income	Declining client base (following compromise of customer lists, credit ratings, preferences, etc.)

Moving From Management Concerns to Responsibilities of the IT Professional

Fiduciary Responsibilities → - Due Diligence - Liability → - Defined Policies and Procedures - Demonstrable Progress

ISSEA
International Systems Security Engineering Association

Business Measures

Potential Indicators of Customer Satisfaction, Flexibility and Productivity	
Customer Satisfaction	License renewal rate Number of new licenses Revenue per customer Number of new customers Number of complaints Customer ratings of products or services (from surveys)
Flexibility	Quoted lead times On-time delivery Time to market Time to accommodate design changes Number of change requests honored Number of common processes
Productivity	Reductions in product development or service cost Rework as a percent of total work Cost-to-revenue ratios Ratios of development time to product life

ISSEA
International Systems Security Engineering Association

Practitioners Guide

- Intended for systems security engineering professionals
- Provides some perspectives for process measurement and lists several desired qualities of performance measures
- Defines measurable entities and associated measurable attributes for software processes
- Identifies a number of specific metrics for each of the SSE-CMM process areas

ISSEA
International Systems Security Engineering Association

Perspectives of Process Measurement

- Performance
- Stability
- Compliance
- Capability
- Improvement and investment

ISSEA
International Systems Security Engineering Association

Process Performance Measures Should:

- Relate closely to the issue under study
- Have high information content
- Pass a reality test
- Permit easy economical collection of data
- Permit consistently collected, well defined data
- Show measurable variation
- As a set, have diagnostic value

ISSEA
International Systems Security Engineering Association

Measurable Entities in a Software Process

- Things received or used
- Activities and their elements
- Things consumed, i.e. resources
- Things held or retained
- Things produced

ISSEA
International Systems Security Engineering Association

Measurable Attributes of Software Process Entities: Things Received or Used

- **Changes:** type, date, size, # received
- **Requirements:** requirements stability, # identified, % traced to design, % traced to code
- **Problem Reports:** type, date, origin, severity
- **Funds:** money, budget, status
- **People:** years of experience, type of education, % trained in XYZ system, employment codes
- **Facilities and Environment:** square feet per employee, # of staff in cubicles, investment in tools per employee, hours of computer usage, % of capacity utilized

ISSEA
International Systems Security Engineering Association

Mapping of Process Areas to Metrics

- Process Area Title
- Process Area Description
- Base Practices
- Related Metrics

ISSEA
International Systems Security Engineering Association

Process Area 8: Monitor System Security Posture

- **Process Area Description:** Ensure that all breaches of, attempted breaches of, or mistakes that could potentially lead to a breach of security are identified and reported.
- **Base Practices:**
  - Analyze event records
  - Monitor changes
  - Identify security incidents
  - Monitor security safeguards
  - Review security posture
  - Manage security incident response
  - Protect security monitoring artefacts

ISSEA
International Systems Security Engineering Association

Process Area 8: Monitor System Security Posture

- **Related Metrics:**
  - number of false positives
  - number of false negatives
  - number of incidents reported
  - number of security policy violations this period
  - number of policy exceptions
  - percentage of expired password
  - number of guessed passwords
  - number of incidents
  - cost of monitoring during this period

Research Effort on the Part of the Information Assurance Technology Analysis Center (IATAC)

ISSEA
International Systems Security Engineering Association

Aims of the IATAC Effort

- A means for uniformly monitoring and objectively documenting the organization's security posture
- A means of determining appropriate corrective measures for specific areas that were identified as needing improvement and for justifying investments in those areas
- A means of tracking IA investments and their effectiveness
- An objective way of comparing strategies for deploying security measures and solutions and instituting and implementing security processes, policies, and procedures

ISSEA
International Systems Security Engineering Association

Difference Between Measurements and Metrics

- **Measurements** provide a one-time view of specific measurable parameters and are represented by numbers, weights, or binary statements.
- **Metrics** are produced by taking measurements over time and comparing two or more measurements with a predefined baseline, thus providing a means for interpretation of the collected data.

ISSEA
International Systems Security Engineering Association

Metrics Must Be "SMART"

- **S**pecific
- **M**easurable
- **A**ttainable
- **R**epeatable
- **T**ime-dependent

ISSEA
International Systems Security Engineering Association

Metrics Development Methodology

Embodies:

- DoD IT Performance Assessment Methodology
- Stakeholder-Based Model
- IA Capabilities-Based Model

ISSEA
International Systems Security Engineering Association

DoD IT Performance Assessment Methodology

Three-Tier Framework:

- IA Capabilities – addresses mission-level capabilities
- Attribute Level – addresses the requirements that support that mission
- Specific Metrics – address specific measurable activities that support those mission requirements

ISSEA
International Systems Security Engineering Association

Stakeholder-Based Model

Views IA metrics from an organizational role perspective:

- Program Manager
- Funding Sponsor
- Senior Security Manager
- Operational User

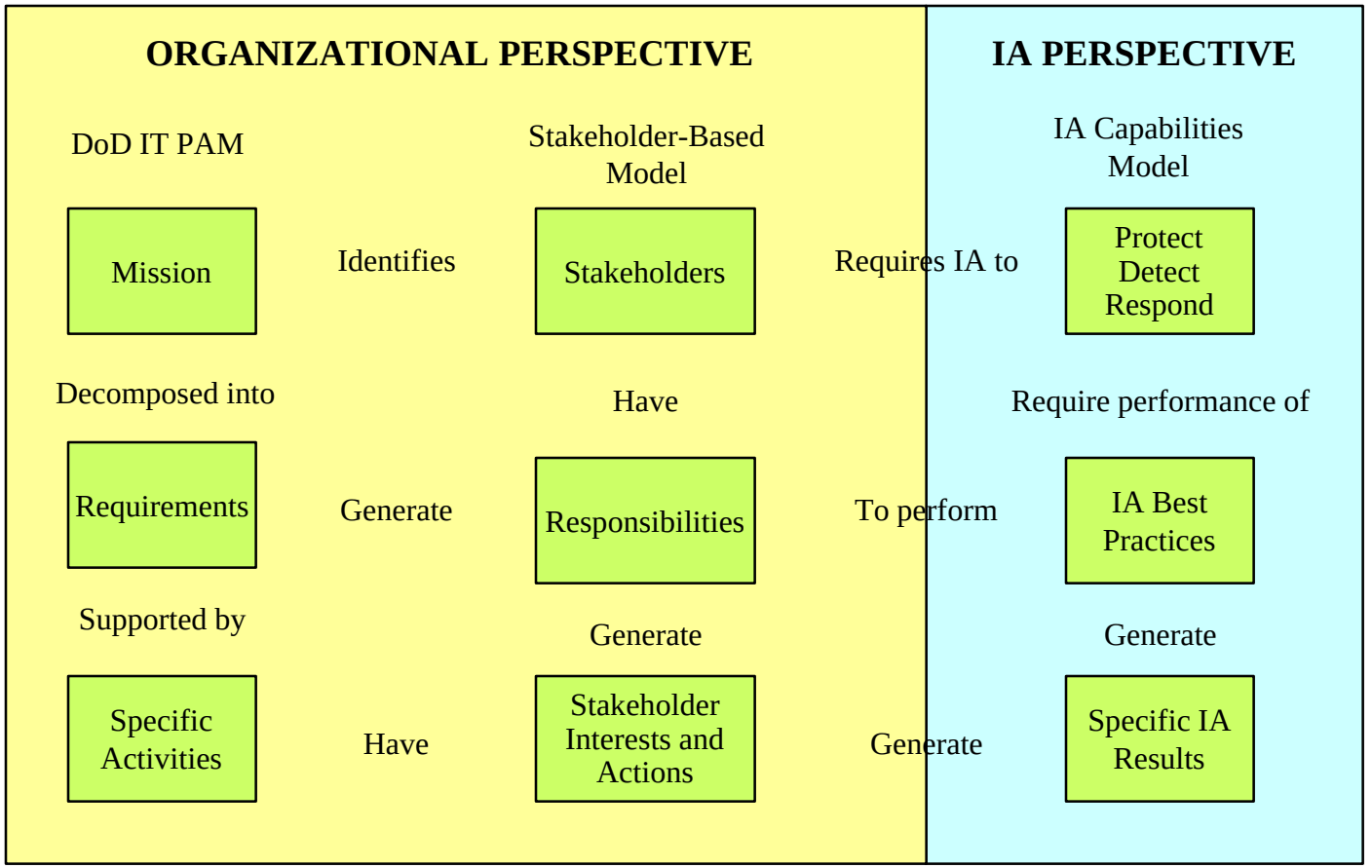
ISSEA
International Systems Security Engineering Association

Capabilities-Based Model

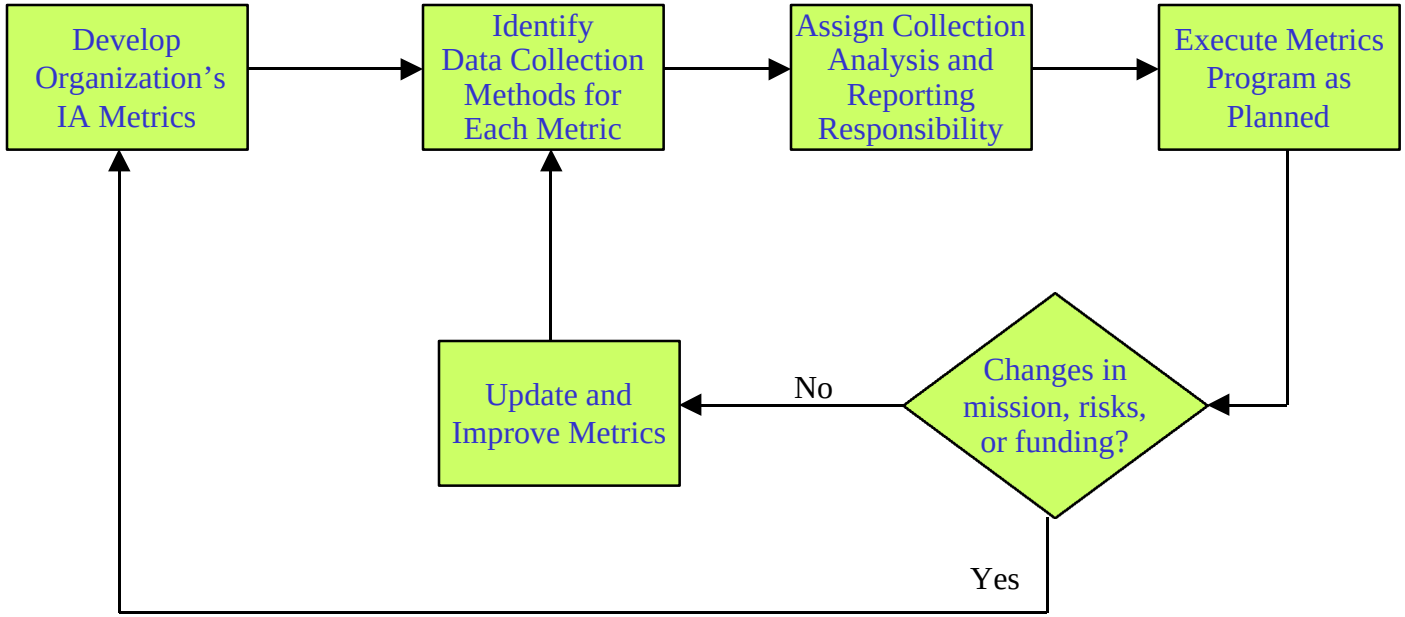
Addresses the functional IA capabilities:

- Protect
- Detect
- Respond

IA Metrics Development Methodology



IA Program Establishment Process



ISSEA
International Systems Security Engineering Association

The IATAC Report

- Outlines an organization-specific metrics development process
- Lists a number of source documents and tools
- Presents and describes a sample IA metrics database

ISSEA
International Systems Security Engineering Association

Data Collection Methods

- Automated tools
- Document review
- Survey and interviews
- System configuration verification
- Observation

ISSEA
International Systems Security Engineering Association

Observations and Conclusions

- Developing metrics requires substantial discipline and commitment
- Meaningful results accrue only if
  - Performance is measured repeatedly over time
  - Metrics are actively used to drive process improvement

ISSEA
International Systems Security Engineering Association

Current State of Security Metrics Research

- Security metrics research is a very hot topic
- Yet, funding is extremely hard to obtain
- Most current effort is unfunded
- Therefore, progress is quite slow
- Much of the current effort tends to be preliminary and somewhat superficial
  - Each environmental setting is different, making it hard to generalize
  - There isn't the support to go deeper